Department of Defense Class 3 Public Key Infrastructure Interface Specification

Version 1.2

10 August 2000

Table of Contents

List of Figures

List of Tables

Section 1

Introduction

This profile describes the interfaces to the DOD CLASS 3 PKI needed by users and applications developers. Use of the common PKI provides economy of scale and allows greater interoperability. The PKI supports economy of scale by providing a single common infrastructure instead of multiple, potentially overlapping or redundant infrastructure if each application or functional community provided their own PKI. Use of a common PKI supports interoperation between applications because the communities share the same PKI.

This profile is an update to a Functional Specification for the DOD PKI released in October 1998[1]. The DOD PKI has evolved since the Functional Specification was written and the profile has changed accordingly. Some of the major changes include greater harmony with the Internet Engineering Task Force (IETF) Public Key Infrastructure Exchange (PKIX) profile, evolution to version 2 Certificate Revocation Lists (CRLs), support for additional types of certificates (such as separate digital signature and encrypting keys and their associated certificates, and additional server certificates), and support of additional protocols such as Certificate Request Message Format (CRMF). It should be noted that over 50,000 certificates have been issued already using the profile in the 1998 specification and developers are referred to that document for ensuring backward compatibility.

It is important that the DOD PKI be compatible with PKI efforts established in other parts of the Federal Government as well as those in the commercial world. This document establishes a profile that is largely the same as the PKIX profile and the Federal PKI (FPKI) profile. In the Certificate and CRL profiles, the DOD profile is listed alongside the other two and footnotes are included to explain the reason for any differences.

This specification provides information for working with the DOD PKI. A set of Interim External Certificate Authorities (IECAs) operated by commercial entities has been approved to provide certificates for contractors and trading partners that do business with the DOD. A separate specification (based on the earlier DOD Functional Specification) applies to the IECAs. It can be found at the IECA web page, http://www.disa.mil/infosec/pkieca/documents.html

[1] Defense Information Infrastructure (DII) Public Key Infrastructure (PKI), Functional Specification (DRAFT), Version: 0.3, October 1998, Defense Information Systems Agency.

To ensure interoperability, DISA has established a test site at the Joint Interoperability Test Center (JITC). For information on how to obtain test certificates from this environment you may contact Ms. Cammie Webster at websterc@fhu.disa.mil or Mr. Gary Baratta at barattag@fhu.disa.mil.   Ms. Webster can also be contacted at (520) 538-5485 or DSN 879-5485.

This document will continue to evolve as standards change. The DOD is committed to the use of commercial standards and evolving as those commercial standards evolve.

Section 2

Certificate Profiles

Many applications may rely on the PKI. Not all of the applications are currently known. However, based on known and anticipated needs, the PKI will issue standard certificates intended to meet these needs. Table 2-1 lists these certificates and their respective purposes and characteristics.

Table 2-1. Standard Certificates

Certificate	Purposes	Characteristics
Identity	Owner authentication Owner accountability (non-repudiation)	Holds only basic, static identity information Private key under owner's exclusive control
E-mail	Separate keys and certificates for signing and encrypting e-mail	Includes e-mail address (non-static) Private encryption key will be escrowed
Server or device	Support Secure Sockets Layer for client-server communications (authentication and privacy) and other services	May include host name or IP address Private key will not be escrowed
IPSEC	Support Internet Protocol Security employment (authentication and privacy) (future)	May include host name or IP address Private key will not be escrowed
Developer	Digitally sign code objects (future)	Identifies development organization Private key under owner's exclusive control

2.1 Certification Authority Certificates

The PKI will employ certificates that follow the X.509 Version 3 (v3) standard. This section describes the certificate fields and standard extensions that the PKI uses. The PKI will provide several standard certificates. Standard certificates have a specific profile and support large communities of users. IETF RFC 2549 provides additional details on the specific format and content of certificates. X.509v3 and RFC 2549 provide guidance that must be supplemented with choices identified in this profile. Interoperability testing with the JITC test suite will also help ensure interoperability.

In the profiles that follow (represented in tabular form) there are portions from a basic certificate and other portions that are extensions. An extension may be critical or non-critical. If an extension is critical and an application does not recognize or cannot process that extension, the application must reject any transaction that depends on such a certificate. In the following tables, “c=yes” or “c=no” is used to represent “critical” and “non-critical” respectively. In addition, the terms “must be present” or “may be present” dictate whether a CA *must* include the extension as a matter of policy or if a certificate without that extension is acceptable. This may be a matter of DOD policy (for the DOD profile column) or a requirement from the IETF or FPKI depending on where the phrases appear in the table.

2.1.1 Root Certificates

There are two types of CA certificates. The Root CA will issue both types. The first type is for the Root CA itself, and the second type is for the signing CAs that exist at the second level of the certificate hierarchy. The following sections describe these certificates. The Root CA is a basic certificate with the least number of certificate extensions. The Root CA’s certificate is self-signed, (i.e., Root CA is both the certificate issuer and subject). The Root CA issues the certificates for the signing CAs. The signing CAs include the extensions found in the Root CA and some additional extensions.

Table 2-2. Root Certification Authority Certificate Profile

FIELD	DOD Root CA Certificate	PKIX	FPKI
Basic Certificate			
Version	V3 (2)	V3 (2)[2]	V3 (2)
Serial Number	Unique Integer	Unique	Unique Integer
Issuer Signature Algorithm	sha1withRSAEncryption[3]	Permits sha-1WithRSAEncryption among others	Algorithm OID; Permits sha-1WithRSAEncryption and id-dsa-with-sha-1

[2] When extensions are present

FIELD	DOD Root CA Certificate	PKIX	FPKI
Issuer Distinguished Name	X.500 DN: cn=DoD CLASS 3 Root CA, ou=PKI, ou=DoD, o=U.S. Government, c=US, (each RDN is printableString)[4]	Printable string acceptable;UTF8String preferred; mandatory after 2003	X.500 DN, matches Subject DN; each RDN is printableString
Validity Period	20 years from date of issue (UTCTime, Zulu); The notBefore component will be the certificate's issue date. The notAfter component will be midnight on the day ending the duration given in the table.	dates through the year 2049 as UTCTime; certificate validity dates in 2050 or later MUST be encoded as GeneralizedTime	dates through the year 2049 as UTCTime; certificate validity dates in 2050 or later MUST be encoded as GeneralizedTime
Subject Distinguished Name	X.500 DN: cn=DoD CLASS 3 Root CA, ou=PKI, ou=DoD, o=U.S. Government, c=US, [5] (each RDN is each RDN is printableString4) will be unique	DirectoryName format Must be unique	X.500 DN (same as Issuer DN)
Subject Public Key Information	1024 bit RSA key modulus, rsaEncryption	rsaEncryption permitted	Permits RSA or DSA
Issuer Unique Identifier	Not used	Should not be used, but should be recognized by Apps	Omitted
Subject Unique Identifier	Not used	(same as above)	Omitted
Issuer's Signature	sha1WithRSAEncryption	sha1WithRSAEncryption is among acceptable algorithms	RSA or DSA
Standard Extensions			
authority key identifier	Not used (since same as subject key identifier for self signed certificate)	CA MUST support unless self signed	Omitted,self-signed (root)

[3] DoD will use the PKIX algorithm, but will monitor trends to determine if it should migrate to the X9.31 standard, based on commercial acceptance.

[4] DoD will monitor commercial practice and migrate to UTF8 format when appropriate

[5] Note that cn=med CA-<n> is present in certificates issued prior to DOD PKI 2.0

FIELD	DOD Root CA Certificate	PKIX	FPKI
subject key identifier	c=no; 20 byteSHA-1 hash of the binary DER encoding of the Root CA's public key information	C=no; CA MUST support, 20 byteSHA-1 hash is one of two acceptable mechanisms	c=no; Must be Included; SHA-1 hash of the certificate's public key
key usage	Not used	C= not specified; CA MUST support, no restriction on combinations	Self-signed (root) must not support
Extended key usage	Not used	C=yes or no; Permitted	Omitted
Private key usage period	Not used	C=no; Recommends against using	Omitted
Certificate policies	Not used	C= not specified; Recommends using OID only.	Omitted
Policy Mapping	Not used (since cross certification is not supported)	C=no; Permitted	Omitted
subject Alternative Name	Not used	Permitted, CA MUST support if subject field empty	Omitted
Issuer Alternative Name	Not used	C=no; Permitted	Omitted
Subject Directory Attributes	Not used	C=no; Permitted, not recommended	Omitted

Basic Constraints	c=no[6];
	cA=True;
	no path length constraint
		C=yes; CA MUST support	c=no for self-signed;
			cA=True
			Pathlength Is optional

Name Constraints	Not used	C=no; not used in self-signed certificates[7]	Omitted
Policy Constraints	Not used	C=yes or no; MUST have either inhibitPolicyMapping field or the requireExplicitPolicy field	Omitted
CRL Distribution Points	Not used since Root's CRL will be short.	C=no; Recommended, note that absence of CRL Issuer means CRL must be issued by CA that signed cert	Omitted
Private Internet Extensions			
Authority Information Access	Not used	C=no; May be included where online validation services are used	Omitted

[6] The decision to make Basic Constraints non-critical for the Root CA was based on a desire to ensure that applications would not reject the root if they could not process Basic Constraints.

[7] Name constraints are not applied to certificates whose issuer and subject are identical.

2.1.2 Signing CA Certificates

Table 2-3. Signing Certification Authority Certificate Profile

FIELD	DOD Signing CA Certificate	PKIX	FPKI
Basic Certificate			
Version	V3 (2)	V3 (2)[8]	V3 (2)
Serial Number	Unique integer	Unique	Unique Integer
Issuer Signature Algorithm[9]	sha1withRSAEncryption	Permits sha-1WithRSAEncryption among others	Algorithm OID; Permits sha-1WithRSAEncryption or id-dsa-with-sha-1
Issuer Distinguished Name	X.500 DN: cn=DoD CLASS 3 Root CA, ou=PKI, ou=DoD, o=U.S. Government, c=US, (each RDN is printableString)[10]	Printable string acceptable;UTF8String preferred; mandatory after 2003	X.500 DN; each RDN is printableString
Validity Period	6 years from date of issue (UTCTime, Zulu); The notBefore component will be the certificate's issue date. The notAfter component will be midnight on the day ending the duration given in the table.	dates through the year 2049 as UTCTime; certificate validity dates in 2050 or later MUST be encoded as GeneralizedTime	dates through the year 2049 as UTCTime; certificate validity dates in 2050 or later MUST be encoded as GeneralizedTime
Subject Distinguished Name[11]	X.500 DN: For identity certificates: cn=DOD CLASS 3 CA-<n>, ou=PKI, ou=DoD, o=U.S. Government, c=US, (each RDN is printableString)[12] For email certificates: cn= DOD CLASS 3 EMAIL CA-<n>, ou=PKI, ou=DoD, o=U.S. Government, c=US, (each RDN is printableString)	DirectoryName format Must be unique	X.500 DN; each RDN is printableString

[8] When extensions are present

[9] DoD will use the PKIX algorithm, but will monitor trends to determine if it should migrate to the X9.31 standard, based on commercial acceptance.

[10] DoD will monitor commercial practice and migrate to UTF8 format when appropriate

[11] Note that cn=med CA-<n> is present in certificates issued prior to DOD PKI 2.0

FIELD	DOD Signing CA Certificate	PKIX	FPKI
Subject Public Key Information	1024 bit RSA key modulus, rsaEncryption	rsaEncryption permitted	RSA or DSA
Issuer Unique Identifier	Not used	Should not be used, but should be recognized by Apps	Omitted
Subject Unique Identifier	Not used	(same as above)	omitted
Issuer's Signature	sha1WithRSAEncryption	sha1WithRSAEncryption is among acceptable algorithms	SHA-1WithRSAEncryption or id-dsa-with-sha-1
Standard Extensions			
authority key identifier	c=no; must be present, 20 byte SHA-1 hash of the binary DER encoding of the Root CA's public key information	C=no; CA MUST support unless self signed, 20 byteSHA-1 hash is one of two acceptable mechanisms	c=no;SHA-1 hash of the public key
subject key identifier	c=no; must be present, 20 byte SHA-1 hash of the binary DER encoding of the subject's public key information	C=no; CA MUST support, 20 byte SHA-1 hash is one of two acceptable mechanisms	c=no; SHA-1 hash of the public key
key usage	c=yes; digitalSignature[13], keyCertSign, cRLSign	C= not specified; CA MUST support, no restriction on combinations	C=yes; Restrictions on combinations[14]
Extended key usage	Not used	C=yes or no; Permitted	Omitted
Private key usage period	Not used	C=no; Recommends against using	Omitted
Certificate policies	c=no[15]; id-US-dod-class3[16] id-US-dod-class3hardware reserved[17] No policy qualifiers[18]	C= not specified; Recommends using OID only.	C=yes; OID ; policyQualifier-URI for CPS, displayText

[12] DoD will monitor commercial practice and migrate to UTF8 format when appropriate

[13] The digital signature is included for cases where the CA must authenticate to other entities, e.g., a directory.

[14] Any combination of digitalSignature, nonRepudiation, cRLSign, keyCertSign permitted

[15] Certificate Policies is non-critical to permit broadest client support.

[16] Note that id-US-medium-pilot is present in certificates issued prior to DOD PKI 2.0

[17] A policy OID has been reserved for future use. It will not be populated in end-entity certificates at this time.

[18] No value seen in pointing to display text.

FIELD	DOD Signing CA Certificate	PKIX	FPKI
Policy Mapping	Not used	C=no; Permitted	C=no Permitted for cross certification
subject Alternative Name	Not used	Permitted, CA MUST support if subject field empty	C=no Permitted; IA5String
Issuer Alternative Name	c=no, URI of directory entry of Root	C=no; Permitted	C=no; permitted, IA5String for DNSName or URI, each RDN is printableString for directoryName
Subject Directory Attributes	Not used	C=no; Permitted, not recommended	Permitted ; for access control based on SDN.706

Basic Constraints	c=yes;
	cA=True;
	no path length constraint
		C=yes; CA MUST support	C=yes for CA;
			cA=True
			Pathlength Is optional

Name Constraints	Not used[19]	C=no	C=yes Recommended, DN or URI
Policy Constraints	c=no[20]; requireExplicitPolicy set with skipCerts set to zero, inhibitPolicyMapping.	C=yes or no; MUST have either inhibitPolicyMapping field or the requireExplicitPolicy field	C=yes; Permit policy mapping, requireExplicitPolicy and inhibitPolicyMapping supported

[19] The DOD does not require names of entities to match the names of the CAs

[20] Policy constraints is non-critical to permit broadest client support

FIELD	DOD Signing CA Certificate	PKIX	FPKI
CRL Distribution Points	c=no; distribution point = URI of directory entry of CA; all reason codes, CRL issuer is CA:[21] e.g., ldap://ds-3.c3pki. chamb.disa.mil/ cn=DOD CLASS 3 Root CA, ou=PKI, ou=DOD, ou=U.S. Government, c=US?certificateRevocationList;binary[22]	C=no; Recommended, note that absence of CRL Issuer means CRL must be issued by CA that signed cert	Allows c=no or yes depending on method of revocation RI and reason codes for that URI, keyCompromise or cACompromise
Private Internet Extensions			
Authority Information Access	Not used	C=no; May be included where online validation services are used	Omitted

[21] Use of a single distribution point for all reasons is intended as a transitional implementation. Future implementations may partition the CRL by reason and store the at separate distribution points.

[22] Actual encoding would be:
ldap://ds-3.c3pki.chamb.disa.mil/cn%3dDoD%20CLASS%203%20CA-3%2cou%3d
PKI%2cou%3dDoD%2co%3dU.S.%20Government%2cc%3dUS?certificateRevocationList%3bbinary

2.2 Server Certificates

Server certificates primarily support the use of secure web applications using SSL. SSL relies on the server key to exchange a symmetric session key. Servers initiating SSL sessions with other servers may also need to authenticate using a digital signature key.

Table 2-4. Standard Server Certificate Profiles

FIELD	DOD Server Certificate	PKIX	FPKI[23]
Basic Certificate			
Version	V3 (**2**)	V3 (2)[24]	V3 (2)
Serial Number	Unique integer	Unique	Integer
Issuer Signature Algorithm[25]	sha-1WithRSAEncryption	Permits sha-1WithRSAEncryption among others	Algorithm OID, Permits sha-1WithRSAEncryption or id-dsa-with-sha-1
Issuer Distinguished Name [26]	X.500 DN: DOD CLASS 3 CA-<n>, ou=PKI, ou=DoD, o=U.S. Government, c=US (each RDN is printableString)[27]	Printable string acceptable;UTF8String preferred; mandatory after 2003	X.500 DN, each RDN is printableString
Validity Period	3 years from date of issue: (UTCTime, Zulu); The notBefore component will be the certificate's issue date. The notAfter component will be midnight on the day ending the duration given in the table.	dates through the year 2049 as UTCTime; certificate validity dates in 2050 or later MUST be encoded as GeneralizedTime	dates through the year 2049 as UTCTime; certificate validity dates in 2050 or later MUST be encoded as GeneralizedTime
Subject Distinguished Name	X.500 DN: cn=<host address>, ou=<C/S/A>, ou=PKI, ou=DoD, o=U.S. Government, c=US (each RDN is printableString)[28]	DirectoryName format Must be unique	X.500 DN, each RDN is printableString

[23] FPKI distinguishes between End Entity and Key Management certificates, but does not distinguish server and user certificates.

[24] When extensions are present

[25] DoD will use the PKIX algorithm, but will monitor trends to determine if it should migrate to the X9.31 standard, based on commercial acceptance.

[26] Note that cn=med CA-<n> is present in certificates issued prior to DOD PKI 2.0

[27] DoD will monitor commercial practice and migrate to UTF8 format when appropriate

[28] DoD will monitor commercial practice and migrate to UTF8 format when appropriate

FIELD	**DOD Server Certificate**	**PKIX**	**FPKI**[23]
Subject Public Key Information	1024 bit RSA key modulus, **rsaEncryption**	rsaEncryption permitted	RSA or DSA
Issuer Unique Identifier	Not used	Should not be used, but should be recognized by Apps	Omitted
Subject Unique Identifier	Not used	(same as above)	Omitted
Issuer's Signature	**sha1WithRSAEncryption**	sha-1WithRSAEncryption is among acceptable algorithms	RSA or DSA
Extensions			
authority key identifier	c=no; must be present, 20 byte SHA-1 hash of the binary DER encoding of the signing CA's public key information	C=no; MUST be supported, 20 byteSHA-1 hash is one of two acceptable mechanisms	C=no; SHA-1 hash of the certificate's public key
subject key identifier	c=**no**; must be present, 20 byte SHA-1 hash of the binary DER encoding of the subject's public key information	C=no; CA MUST support, 20 byteSHA-1 hash is one of two acceptable mechanisms	C=no; SHA-1 hash of the certificate's public key
key usage	c=yes; keyEncipherment, digitalSignature[29]	no restriction on combinations	C=yes; must be included, Restrictions on combinations[30]
Extended key usage	Not used[31]	C=yes or no; Permitted	Omitted
Private key usage period	Not used	C=no; Recommends against using	Omitted
Certificate policies	c=no[32]; id-US-dod-class3[33] No policy qualifiers[34]	C= not specified, Recommends using OID only.	C=yes OID, URI of CPS, DisplayText permitted
Policy Mapping	Not used	C=no; Permitted	Omitted

[29] Since many products do not currently support separate signing and key exchange keys, use of the same key for both is being permitted. There are no current requirements for non-repudiation in servers, which is helpful since the same certificate could not support both non-repudiation and key exchange.

[30] Key encipherment for key management; a combination of digitalSignature, nonRepudiation is permitted for EE certs.

[31] Exteneded key usage may be supported in the future for end entity certificates

[32] Certificate Policies is non-critical to permit broadest client support.

[33] Note that id-US-medium-pilot is present in certificates issued prior to DOD PKI 2.0

[34] No value seen in pointing to display text.

FIELD	DOD Server Certificate	PKIX	FPKI[23]
subject Alternative Name	Not used	Permitted, CA MUST support if subject field empty; may be IP Address or DNS Name	C=no, permitted, DNSName, DN, or URI
Issuer Alternative Name	URI of CA's directory entry	C=no; Permitted	C=no, permitted, DNSName, DN, or URI
Subject Directory Attributes	Not used	C=no; Permitted, not recommended	C=no;Permitted ; recommends using SDN.706
Basic Constraints	Not used in EE certificates[35]	This extension SHOULD NOT appear in end entity certificates	C=yes, CA=false
Name Constraints	Not used[36]	Not permitted in EE certs	OmittedNot in EE certs
Policy Constraints	Not used	Not permitted in EE certs	OmittedNot in EE certs
CRL Distribution Points	c=**no**; distribution point = URI of directory entry of CA that issued this certificate; all reason codes, CRL issuer is CA [37]	C=no; Recommended, note that absence of CRL Issuer means CRL must be issued by CA that signed cert	Allows c= yes; URI and reason codes for that URI: keyCompromise, affiliationChanged, cessationOfOperation
Private Internet Extensions			
Authority Information Access	Not used	C=no; May be included where online validation services are used	Omitted

[35] Previous releases of the DOD PKI permitted basic constraints in EE certificates with CA=false as used in the FPKI. At the time of this draft, the DOD has chosen to conform to the PKIX standard which appears to be an industry consensus.

[36] The DOD does not require names of entities to match the names of the CAs

[37] Actual encoding would be:
ldap://ds-3.c3pki.chamb.disa.mil/cn%3dDoD%20CLASS%203%20CA-3%2cou%3d PKI%2cou%3dDoD%2co%3dU.S.%20Government%2cc%3dUS?certificateRevocationList%3bbinary

2.3 User Certificates

The identity certificate is normally for people and is the electronic equivalent of an ID card. This certificate contains limited, relatively static information. It does not include more dynamic information such as detailed organizational affiliation and e-mail address. The subject name in the certificate is the DN for a corresponding entry in the directory.

2.3.1 Identity Certificates

Table 2-5. Standard User Identity Certificate Profile

FIELD	DOD Identity Certificate	PKIX	FPKI
Basic Certificate			
Version	V3 (2)	V3 (2)[38]	V3 (2)
Serial Number	Unique integer	Unique	Integer
Issuer Signature Algorithm[39]	sha1WithRSAEncryption	Permits sha-1WithRSAEncryption among others	Algorithm OID; Permits sha-1WithRSAEncryption or id-dsa-with-sha-1
Issuer Distinguished Name	X.500 DN: cn=DOD CLASS 3 CA-<n>, ou=PKI, ou=DoD, o=U.S. Government, c=US [40] (each RDN is printableString)[41]	Printable string acceptable;UTF8String preferred; mandatory after 2003	X.500 DN, each RDN is printableString

[38] When extensions are present

[39] DoD will use the PKIX algorithm, but will monitor trends to determine if it should migrate to the X9.31 standard, based on commercial acceptance.

[40] Note that cn=med CA-<n> is present in certificates issued prior to DOD PKI 2.0

[41] DoD will monitor commercial practice and migrate to UTF8 format when appropriate

FIELD	DOD Identity Certificate	PKIX	FPKI
Validity Period	3 years from date of issue (UTCTime, Zulu); The notBefore component will be the certificate's issue date. The notAfter component will be midnight on the day ending the duration given in the table.	dates through the year 2049 as UTCTime; certificate validity dates in 2050 or later MUST be encoded as GeneralizedTime	dates through the year 2049 as UTCTime; certificate validity dates in 2050 or later MUST be encoded as GeneralizedTime
Subject Distinguished Name	X.500 DN: cn=<name>[42], ou=<C/S/A>, ou=PKI, ou=DoD, o=U.S. Government, c=US [43]	DirectoryName format Must be unique Email address is deprecated	X.500 DN, each RDN is printableString
Subject Public Key Information	1024 bit RSA key modulus, rsaEncryption	rsaEncryption permitted	RSA or DSA
Issuer Unique Identifier	Not used	Should not be used, but should be recognized by Apps	Omitted
Subject Unique Identifier	Not used	(same as above)	Omitted
Issuer's Signature	sha-1WithRSAEncryption	sha-1WithRSAEncryption is among acceptable algorithms	RSA or DSA
Standard Extensions			
authority key identifier	c=no; must be present, 20 byte SHA-1 hash of the binary DER encoding of the signing CA's public key information	C=no; MUST be included in end-entity certificates, 20-byteSHA-1 hash is one of two acceptable mechanisms	C=no; SHA-1 hash of the certificate's public key

[42] In user certificates issued by the DOD, the entire common name will not exceed 64 characters and will be unique. Applications should not assume a particular format for the common name. In current certificates, the common name consists of last name, generational qualifier, first name or initial, middle name or initial, and a ten-digit number, separated by periods; e.g., Smith.Jr.John.A.1234567890. Future releases may move the unique number to a separate attribute and make other changes to the format.

[43] DoD will monitor commercial practice and migrate to UTF8 format when appropriate

FIELD	DOD Identity Certificate	PKIX	FPKI
subject key identifier	c=no; must be present, 20 byte SHA-1 hash of the binary DER encoding of the subject's public key information	C=no; SHOULD be included in end-entity certificates, 20 byte SHA-1 hash is one of two acceptable mechanisms	C=no; must be Included, SHA-1 hash of the certificate's public key

key usage	c=yes; digitalSignature, nonRepudiation	CA MUST support, no restriction on combinations	C=yes
			Must be included;
			Restrictions on combinations[44]

Extended key usage	Not used[45]	C=yes or no; Permitted	Omitted
Private key usage period	Not used	C=no; Recommends against using	Omitted
Certificate policies	c=no[46]; id-US-dod-class3[47] or id-US-dod-class3hardware No policy qualifiers[48]	C= unspecified; Recommends using OID only.	C=yes OID, URI of CPS, DisplayText permitted
Policy Mapping	Not used	C=no; Permitted	Omitted
subject Alternative Name	Not used	Permitted, CA MUST support if subject field empty	C=no, permitted, DN[49]
Issuer Alternative Name	C=no; URI of CA's directory entry in IA5String format e.g., ldap://ds-3. c3pki.chamb.disa.mil/cn= DOD CLASS 3 CA-<n>, ou=PKI,ou=DOD, ou=U.S. Government,c=US[50]	C=no; Permitted	C=no Permitted, DNSName, DN, or URI

[44] A combination of digitalSignature and nonRepudiation is permitted

[45] Exteneded key usage may be supported in the future for end entity certificates

[46] Certificate Policies is non-critical to permit broadest client support.

[47] Note that id-US-medium-pilot is present in certificates issued prior to DOD PKI 2.0

[48] No value seen in pointing to display text.

[49] Note that FPKI does not distinguish between user and server end entities. DNSName and URI do not make sense for users and are omitted here although they appear in the FPKI EE profile

[50] Actual encoding:
ldap://ds-3.c3pki.chamb.disa.mil/cn%3dDoD%20CLASS%203%20CA-3%2cou%3d PKI%2cou%3dDoD%2co%3dU.S.%20Government%2cc%3dUS; the purpose is to aid in obtaining a certificate chain by pointing to the directory entry where the certificate is stored.

FIELD	DOD Identity Certificate	PKIX	FPKI
Subject Directory Attributes	Not currently used	C=no; Permitted, not recommended	Permitted ; recommends using SDN.706access controls
Basic Constraints	Not used[51]	This extension SHOULD NOT appear in end entity certificates	C=yes; CA=false
Name Constraints	Not used	Not permitted for EE certs	Omitted
Policy Constraints	Not used	Not permitted for EE certs	Omitted
CRL Distribution Points	c=**no**; distribution point = URI of directory entry of CA; all reason codes, CRL issuer is CA:[52] e.g., ldap://ds-3.c3pki.chamb. disa.mil/ cn=DOD CLASS 3 CA-<n>, ou=PKI, ou=DOD, ou=U.S. Government, c=US?certificateRevocationList;binary[53]	C=no; Recommended, note that absence of CRL Issuer means CRL must be issued by CA that signed cert	Allows c=yes; URI and reason codes for that URI; keyCompromise, affiliationChanged, cessationOfOperation
Private Internet Extensions			
Authority Information Access	Not used	C=no; May be included where online validation services are used	Omitted

2.3.2 E-mail Certificate

The purpose of e-mail certificates is to enable the associated subscriber to use S/MIME email. S/MIME e-mail provides capability to send either or both signed and encrypted e-mail. There will be two versions of e-mail certificate. One version is for the verification of signed messages that the subscriber sends, and the other is for the encryption of symmetric message keys for messages the subscriber receives. S/MIME e-mail certificates must include the

[51] Previous releases of the DOD PKI permitted basic constraints in EE certificates with CA=false as used in the FPKI. At the time of this draft, the DOD has chosen to conform to the PKIX standard which appears to be an industry consensus.

[52] Use of a single distribution point for all reasons is intended as a transitional implementation. Future implementations may partition the CRL by reason and store the at separate distribution points.

[53] Actual encoding would be:
ldap://ds-3.c3pki.chamb.disa.mil/cn%3dDoD%20CLASS%203%20CA-3%2cou%3d
PKI%2cou%3dDoD%2co%3dU.S.%20Government%2cc%3dUS?certificateRevocationList%3bbinary

certificate owner's e-mail address. A user's email address is contained in the subject alternative name extension. Note that this is a change from the DOD PKI version 1.0 which placed the email address in an "E=" attribute in the subject distinguished name.

Table 2-6. Standard Email Certificate Profile

FIELD	DOD E-mail Certificate	PKIX	FPKI
Basic Certificate			
Version	V3 (2)	V3 (2)[54]	V3 (2)
Serial Number	Unique integer	Unique	Integer
Issuer Signature Algorithm	sha1WithRSAEncryption[55]	Permits sha-1WithRSAEncryption among others	Algorithm OID; Permits sha-1WithRSAEncryption or id-dsa-with-sha-1
Issuer Distinguished Name [56]	X.500 DN: cn=DOD CLASS 3 EMAIL CA-<n>, ou=PKI, ou=DoD, o=U.S. Government, c=US (each RDN is printableString)[57]	Printable string acceptable;UTF8String preferred; mandatory after 2003	X.500 DN, each RDN is printableString
Validity Period	2 years from date of issue (UTCTime, Zulu); The notBefore component will be the certificate's issue date. The notAfter component will be midnight on the day ending the duration given in the table.	dates through the year 2049 as UTCTime; certificate validity dates in 2050 or later MUST be encoded as GeneralizedTime	dates through the year 2049 as UTCTime; certificate validity dates in 2050 or later MUST be encoded as GeneralizedTime
Subject Distinguished Name	X.500 DN: <name>,[58] [59] ou=<C/S/A>, ou=PKI, ou=DoD, o=U.S. Government, c=US [60]	DirectoryName format Must be unique Email address is deprecated	X.500 DN, each RDN is printableString

[54] When extensions are present

[55] Current product bug may force use of MD5 signatures on Key Exchange certs

[56] Note that cn=med CA-<n> is present in certificates issued prior to DOD PKI 2.0

[57] DoD will monitor commercial practice and migrate to UTF8 format when appropriate

[58] In user certificates issued by the DOD, the entire common name will not exceed 64 characters and will be unique. Applications should not assume a particular format for the common name. In current certificates, the common name consists of last name, generational qualifier, first name or initial, middle name or initial, and a ten-digit number, separated by periods; e.g., Smith.Jr.John.A.1234567890. Future releases may move the unique number to a separate attribute and make other changes to the format.

FIELD	DOD E-mail Certificate	PKIX	FPKI
Subject Public Key Information	1024 bit RSA key modulus, rsaEncryption	rsaEncryption permitted	RSA or DSA
Issuer Unique Identifier	Not used	Should not be used, but should be recognized by Apps	Omitted
Subject Unique Identifier	Not used	(same as above)	Omitted
Issuer's Signature	sha-1WithRSAEncryption	sha-1WithRSAEncryption is among acceptable algorithms	RSA or DSA
Standard Extensions			
authority key identifier	c=no; 20 byte SHA-1 hash of the binary DER encoding of the signing CA's public key information	C=no; MUST be included in end-entity certificates, 20-byteSHA-1 hash is one of two acceptable mechanisms	C=no; SHA-1 hash of the certificate's public key
subject key identifier	c=no; 20 byte SHA-1 hash of the binary DER encoding of the subject's public key information	C=no; SHOULD be included in end-entity certificates, 20 byte SHA-1 hash is one of two acceptable mechanisms	C=no; must be Included, SHA-1 hash of the certificate's public key
key usage	c=yes; email signing certificate[61]: digitalSignature and non-repudiation email key exchange certificate: keyEncipherment	CA MUST support, no restriction on combinations	C=yes Restrictions on combinations[62]
Extended key usage	Not used[63]	C=yes or no; Permitted	Omitted
Private key usage period	Not used	C=no; Recommends against using	Omitted

[59] In DOD PKI release 1.0, the user's email address appeared as an "E=" attribute in the DN; in release 2.0, the email address is in subjectAltName

[60] DoD will monitor commercial practice and migrate to UTF8 format when appropriate

[61] Because many S/MIME clients do not enforce functional separation both the digitalSignature and keyEncipherment flags may be set in older certificates. However, since S/MIME clients that enforce functional separation the PKI are beginning to become available, the DOD PKI 2.0 will issue one S/MIME certificate with the digital signature and non-repudiation bits set and a second certificate with the key encipherment bit set.

[62] Key encipherment or key agreement permitted in KM certs, digitalSignature and nonRepudiation are permitted in DS certs.

[63] Exteneded key usage may be supported in the future for end entity certificates

FIELD	DOD E-mail Certificate	PKIX	FPKI
Certificate policies	c=no[64]; id-US-dod-class3[65] or id-US-dod-class3hardware No policy qualifiers[66]	C= unspecified; Recommends using OID only.	C=yes; OID, URI of CPS, DisplayText permitted
Policy Mapping	Not used	C=no; Permitted	Omitted
subject Alternative Name	C=no; RFC822 Name[67]	Permitted, CA MUST support if subject field empty	C=no, permitted, DN[68]
Issuer Alternative Name	C=no; URI of CA's directory entry	C=no; Permitted	C=no Permitted, DNSName, DN, or URI
Subject Directory Attributes	Not currently used	C=no; Permitted, not recommended	Permitted ; recommends SDN.706 access controls
Basic Constraints	Not used[69]	This extension SHOULD NOT appear in end entity certificates	C=yes; CA=false
Name Constraints	Not used	Not permitted for EE certs	Omitted
Policy Constraints	Not used	Not permitted for EE certs	Omitted
CRL Distribution Points	c=**no**;[70] distribution point = URI of directory entry of CA; all reason codes, CRL issuer is CA [71]	C=no; Recommended, note that absence of CRL Issuer means CRL must be issued by CA that signed cert	Allows c=no or yes; URI and reason codes for that URI; keyCompromise, affiliationChanged, cessationOfOperation
Private Internet Extensions			

[64] Certificate Policies is non-critical to permit broadest client support.

[65] Note that id-US-medium-pilot is present in certificates issued prior to DOD PKI 2.0

[66] No value seen in pointing to display text.

[67] Use of E= attribute as part of CN may be present in older certificates; note this is a change from DOD PKI release 1.0

[68] Note that FPKI does not distinguish between user and server end entities. DNSName and URI do not make sense for users and are omitted here although they appear in the FPKI EE profile

[69] Previous releases of the DOD PKI permitted basic constraints in EE certificates with CA=false as used in the FPKI. At the time of this draft, the DOD has chosen to conform to the PKIX standard which appears to be an industry consensus.

[70] CRL Distribution Point will be omitted initially in PKI 2.0 pending merger of the email and identity directories

[71] Actual encoding would be:
ldap://ds-3.c3pki.chamb.disa.mil/cn%3dDoD%20CLASS%203%20CA-3%2cou%3d
PKI%2cou%3dDoD%2co%3dU.S.%20Government%2cc%3dUS?certificateRevocationList%3bbinary

FIELD	DOD E-mail Certificate	PKIX	FPKI
Authority Information Access	Not used	C=no; May be included where online validation services are used	Omitted

2.4 Developer Certificates (Future)

In the future, the DOD may support developer certificates to help ensure the integrity of downloaded mobile code. The certificate and associated private key will permit software developers or distributors to provide the user with information to determine the source of the software and detect whether the software has been corrupted during distribution. As yet there are no standards for signing software modules. The DOD will monitor industry progress and may support a software signing capability in the future.

Section 3

Certificate Revocation List

Certificate Revocation Lists (CRL) enumerate unexpired certificates that have been revoked or placed on “hold.” In the general case, certificates may be revoked for a variety of reasons. A “hold” indicates the CA will not vouch for the binding of the certificate subject and public key at this time. The DOD PKI will not use the hold feature.

The X.509 v2 certificate revocation list format adds several optional extensions to the v1 format, similar in concept to those defined for certificates. This DOD PKI Release 2.0 uses version 2 CRLs with all extensions set as non-critical. In the future, the CA that issues a CRL is not necessarily the CA that issued the revoked certificate, and some CAs may issue only CRLs.

Reasons for revocation include:

- KeyCompromise – there is reason to believe the token on which a user or other end-entity private key resides or a copy of the private key (in the case of software tokens) has been obtained by an unauthorized individual
- CACompromise – there is reason to believe the token on which the CA private key resides has been obtained by an unauthorized individual
- AffiliationChanged—the user has terminated his/her association with an organization listed in the Distinguished Name in the certificate; position changes within an organization do not require revocation of a certificate
- Superseded—a replacement certificate has been issued to a user, other end-entity, or CA and none of the above reasons are applicable; examples include: the token has failed, the user has forgotten the password to unlock the token, change in legal name, change in unique identifier.
- CessationOfOperation—applies to CA certificates; operation of the CA has been terminated; note that if a CA no longer issues certificates, but remains capable of issuing CRLs, its certificate need not be revoked and certificates issued by the CA may continue to be used
- CertificateHold—a temporary revocation that is not to be used by the DOD PKI

Table 3-1. Certificate Revocation List Profile

FIELD	DOD PKI	PKIX	FPKI[72]
Version (optional)	V2	OPTIONAL, if present, shall be v2 (1)[73]	V2 (1)
Issuer (Distinguished Name)	CA's DN, e.g., cn=DOD CLASS 3 CA-<n>, ou=PKI, ou=DoD, o=U.S. Government, c=US; each RDN is a printableString[74]	an X.500 distinguished name (DN)	Issuer DN
This Update	date this CRL was issued, UTCTime for dates through the year 2049; GeneralizedTime for dates in the year 2050	issue date of this CRL UTCTime for dates through the year 2049; GeneralizedTime for dates in the year 2050 or later	when the CRL was generated
Next Update	date by which the next CRL will be issued; same formats as above, 1 day (24 hours) later than "This Update" for signing CAs, 28 days later for Root	date by which the next CRL will be issued; same formats as above	when the next CRL update will be generated, if a scheduled time is known
Revoked Certificates, a sequence of one or more of the following sequence:[75]			
Certificate Serial Number	CertificateSerialNumber	CertificateSerialNumber	serial number of each revoked certificate
Revocation Date	The date on which the revocation occurred; same format as for update fields	The date on which the revocation occurred; same format as for update fields	revocationDate
CRL Entry Extensions (optional)		if present, certificate shall be v2	crlEntryExtensions field(s)

[72] The FPKI intends to deploy an Indirect CRL signed by a special CA and used only for key compromise and CA compromise. Also note that the FPKI CRL description is from the older, January 1999 profile as opposed to the January 2000 profile

[73] Presence of extensions requires this be set to V2.

[74] DoD will monitor commercial practice and migrate to UTF8 format when appropriate

[75] The sequence must not be present if there are no revoked certificates

FIELD	DOD PKI	PKIX	FPKI[72]
reasonCode	C=no; supported, permitted codes: keyCompromise, cACompromise, affiliationChanged, superseded, cessationOfOperation One of the above codes must be specified in any revocation entry.	C=yes or no; recommended to be included, identifies the reason for the certificate revocation: unspecified, keyCompromise, cACompromise, affiliationChanged, superseded, cessationOfOperation, certificateHold, removeFromCRL	C=no; include CRLReason bits for unspecified, key compromise, CA compromise, affiliation change, superseded, and cessation of operation
holdlinstructionCode	Not used (since hold reason code is not used)	C= yes or no; optional, OID indicating action to be taken after encountering certificate placed on hold	C=no; Not supported
invalidityDate	Not used	C= yes or no; recommended to be included, date on which it is known or suspected that the private key was compromised	C=no; may be included, but no automated processing required
certificateIssuer	not used	C= yes; optional, the certificate issuer associated with an entry in an indirect CRL	C=yes; generated only for ICRL entries, “issuer” Name field of the revoked certificate
CRL Extensions (optional)			
authorityKeyIdentifier	C=no; KeyIdentifier method[76]	C= not specified; must be included, subject key identifier in the CRL signer's certificate;	C=no; must be included, authority key identifier
issuerAltName	not used	C=no; optional, allows additional identities to be associated with the issuer	C=no; DNS Name or URI
cRLNumber	C=no; supported, monotonically increasing sequence number[77]	C=n; must be included, a monotonically increasing sequence number for each CRL issued by a CA	C=no; monotonically increasing sequence number
IssuingDistribution Point	Not used	C=yes; optional, Identifies the CRL distribution point for a particular CRL, and it indicates whether the CRL covers revocation for end entity certificates only, CA certificates only, or a limited set of reason codes	C=yes; issued only for ICRLs
deltaCRLIndicator	not used	C=not specified; optional, identifies a delta-CRL	Not used

[76] Note this attribute is not supported in DOD PKI Release 2.0. It is expected to be supported in future releases.

[77] Note this attribute is not supported in DOD PKI Release 2.0. It is expected to be supported in future releases.

FIELD	DOD PKI	PKIX	FPKI[72]
Signature (Issuer Signature Algorithm)	AlgorithmIdentifier, sha-1WithRSAEncryption permitted	AlgorithmIdentifier, sha-1WithRSAEncryption permitted	algorithm used to certify the CRL (if parameters are associated with the signature algorithm, those parameters shall not be included)
Signature Value	Digital signature computed upon ASN.1 DER encoded CRL (excluding signature algorithm and signature value) ASN.1 encoded as a BIT STRING	Digital signature computed upon ASN.1 DER encoded CRL (excluding signature algorithm and signature value) ASN.1 encoded as a BIT STRING	Present

Section 4

Registration Interfaces

The registration process is used to obtain certificates from the DOD PKI. Currently, three registration interfaces are supported:

- Certificate Request Message Format (CRMF)
- KEYGEN Tag
- PKCS #10

The first two are used for people. Once certificates have been obtained, the certificates and associated private keys may be moved to other applications using PKCS#12. DOD policy requires that cryptographic modules used for generating keys must be evaluated under Federal Information Processing Standards (FIPS) 140-1 and satisfy at least level 2 software module requirements. A draft FIPS 140-2 is currently in development. It is expected that this new FIPS will be required after it has been finalized and products have been evaluated using it.

4.1 Certificate Request Message Format (CRMF)

The Certificate Request Message Format is a proposed Internet standard for requesting certificates from a CA. The following is from RFC 2511:

1. A CertRequest value is constructed. This value may include the public key, all or a portion of the end-entity's (EE's) name, other requested certificate fields, and additional control information related to the registration process.
2. A proof of possession (of the private key corresponding to the public key for which a certificate is being requested) value may be calculated across the CertRequest value.
3. Additional registration information may be combined with the proof of possession value and the CertRequest structure to form a CertReqMessage.
4. The CertReqMessage is securely communicated to a CA.

In the DOD PKI, requests for S/MIME certificates must come from a client capable of CRMF requests and the key escrow feature. The CertReqMessage is a base64 encoded blob posted to the CA using HTTP over SSL. The certReqMessage supports the key escrow function in which the private key associated with the key exchange certificate is encrypted in a transport certificate and forwarded to a key recovery facility operated by the DOD PKI by the CA. The recovery facility automatically decrypts the user's private key, ensures that the public key in the certificate request is part of the same key pair, encrypts the private key using a storage key, stores the encrypted private key, and notifies the CA that the key has been escrowed. Further details can be found in the DOD PKI Release 2.0 CONOPS.

The certificates are automatically incorporated in the user's browser at the end of the process.

4.2 KEYGEN

Another interface is an HTML tag known as KEYGEN embedded in a web page. This method works for certain browsers (e.g., Netscape Navigator), and causes them to generate a key pair and post a certificate request to the CA. This interface will be provided to users who require only ID certificates and whose browsers are not able to use CRMF. The type of browser is detected automatically. The URL for registration can be found in Appendix C.

From the Netscape HTML Tag Reference guide:

"The KEYGEN tag facilitates the generation of key material and submission of the public key as part of an HTML form. This mechanism is designed for use in web-based certificate management systems. It displays a menu of key-size choices from which the user must choose one.

Then, when the submit button is clicked, a key pair of the selected size is generated. The private key is encrypted and stored in the local key database.

The public key and challenge string are DER encoded as **PublicKeyAndChallenge** and then digitally signed with the private key to produce a **SignedPublicKeyAndChallenge**. The **SignedPublicKeyAndChallenge** is base64 encoded, and the ASCII data is finally submitted to the server as the value of a name-value pair, where the name is specified by the NAME attribute of the KEYGEN tag.

Syntax

```
<KEYGEN
  NAME="name"
  CHALLENGE="challenge"
>
```

The NAME attribute is required

NAME="name" specifies the name for the name/value pair."

The CHALLENGE string is not used in the DOD PKI.

4.3 PKCS #10

The third interface is RSA's PKCS #10[78]. This interface within the DOD PKI is intended for certificates issued to machines, such as web servers and some vendor VPN devices. Through a server-specific interface, a public-private key pair is generated. From PKCS #10:

1. "A CertificationRequestInfo value containing a distinguished name, a public key, and a set of attributes is constructed by a server.
2. The CertificationRequestInfo value is signed with the server's private key.
3. The CertificationRequestInfo value, a signature algorithm identifier, and the server's signature are collected together into a CertificationRequest value."

In the DOD PKI, the CertificationRequest value is encoded in base64 format, which is inserted into an HTML form on the CA.[79]

Once approved, the CA creates a certificate in PKCS #7 format (base64 encoded) which may be retrieved from the CA by using a browser. A server-specific interface is used to insert the certificate into the server.

4.4 CMC (Certificate Management Messages over Cryptographic Message Syntax [CMS])

A draft protocol known as CMC (Certificate Management Messages over Cryptographic Message Syntax [CMS]), show promise as a standard for unifying various forms of registration. It will incorporate the CRMF described above as well as Certificate Enrollment Protocol (CEP) which is used by Cisco for registering VPN certificates. DOD will support CMC in the future if appropriate.

[78] RSA Laboratories. PKCS #10: Certification Request Syntax Standard. Version 1.0, November 1993

[79] The HTML form is not part of the PKCS #10 specification, which is silent on the means of transport, but is part of the DOD PKI.

4.5 PKCS#12

RSA’s PKCS#12 is used to move already obtained certificates and private keys into other applications or cryptographic modules.

Section 5

Online Certificate Status Protocol

The Online Certificate Status Protocol (OCSP) is a mechanism that permits online validation of a certificate to ensure that it has not been revoked. In contrast to validation using CRLs, which require the client or server to download the entire list of revoked certificates, OCSP validates only those certificates needed for the transaction. As a result, OCSP transactions will be much smaller but will occur much more frequently than CRL downloads. OCSP responses will contain no information newer than that found in the CRL last published by the corresponding CA.

OCSP will not be supported in the Release 2.0 DOD PKI but is expected to be part of the infrastructure in Release 3.0. At that time, the DOD PKI will support OCSP in *addition* to CRLs (which are stored in the Directory).

From RFC 2560:

An OCSP request is sent to the OCSP responder using the html post method and contains the following data:

1. protocol version
2. service request
3. target certificate identifier
4. optional extensions which MAY be processed by the OCSP Responder

A response consists of:

1. version of the response syntax
2. name of the responder
3. responses for each of the certificates in a request
4. optional extensions
5. signature algorithm OID
6. signature computed across hash of the response

The response for each of the certificates in a request consists of

1. target certificate identifier
2. certificate status value
3. response validity interval
4. optional extensions

The following are permitted response indicators:

1. good
2. revoked
3. unknown

The protocol permits OCSP responses to be signed by the CA that originally issued the certificate or by a specially designated *OCSP Responder.* In the DOD PKI, specially designated responders will be used.

An OCSP Responder’s signing certificate will assert the extended key usage extension, OCSPSigning. Each CA served by an OCSP Responder must issue a certificate to that responder with the OCSPSigning (**id-kp-OCSPSigning**) extension to indicate that the CA authorizes the Responder to validate certificates issued by that CA.

The DOD PKI will **not** support the OCSPNoCheck extension (**id-pkix-ocsp-nocheck**). This extension is an option in the OCSP standard that indicates that the end entity need not obtain a CRL for the OCSP Responder’s signing certificate. In the DOD PKI, the revocation status of the OCSP responder certificates will need to be verified as well as other certificates.

The PKIX standard gives the option of specifying an Authority Information Access (AIA) include an AuthorityInfoAccess extension (**id-pe-authorityInfoAccess**) in a certificate or configuring the address of the responder into clients and applications. The DOD has chosen to use the latter method since it enables static load balancing and permits a particular client or application to access a responder with the best network connectivity.

Section 6

Directory Schema

The directory is based on the X.500 Standards. This section describes the directory organization. The PKI follows the distinguished name conventions. The X.500 naming structure is hierarchical and designed to provide a unique naming structure worldwide based on decentralized control of naming. This section describes the directory hierarchy, the distinguished name conventions for uniquely naming entries in the directory, the allowed directory objects, and the data elements that describe each object.

6.1 Directory Hierarchy

Under the standards process an organization serves to register names at each level of the hierarchy. In order to ensure that the DoD PKI naming structure is unique from other X.500 names, all PKI issued DNs will share a common suffix. This suffix is the base suffix. For the DOD PKI, the base suffix shall be:

<base suffix>= ou=PKI, ou=DoD, o=U. S. Government, c=US

Each successive level of the hierarchy becomes the suffix for the DNs at the next level of the hierarchy. Figure 6-1 illustrates the directory information tree (DIT). There are four levels to the PKI's base suffix. Entries at the next level, the fifth level, shall define DoD organizations at the commander-in-chief (CINC), service, and agency level. The term "Contractor" will appear in certificates issued to contractors in place of a DoD organization. Appendix D lists the organizations at level 5. CAs will also exist at level 5 of the directory and will be the only end-entities at level 5. All other end-entities will be at level 6 and be under their sponsoring organization. In the DoD PKI, CAs are not in the naming structure of the entities whose certificates they sign. Administrative procedures will allocate the association of CAs to RAs and LRAs. Factors such as load balancing and certificate server capacity will determine this association. The association may change. Relying parties should base trust on the Root CA rather than individual CAs.

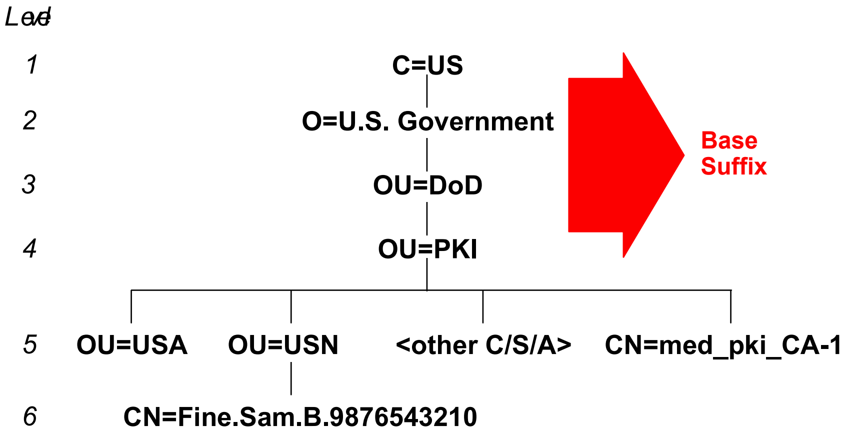

Figure 6-1. DOD PKI Directory Information Tree (DIT)

6.2 Distinguished Names

All distinguished names will share the base suffix. CAs will be at level 5 of the directory. The remainder of this section describes the relative distinguished names (RDNs) of the various PKI entities.

6.2.1 Root CA

The Root CA like all CAs shall be at level 5 of the DIT. The relative DN for the Root CA is:

cn=DoD CLASS 3 Root CA

Thus, the complete DN for the root is:

cn=DoD CLASS 3 Root CA, ou=PKI, ou=DoD, o=U.S. Government, c=US

6.2.2 Signing CAs

The signing CAs shall also be at level 5 of the DIT. The relative DN for the signing CA is:

cn=DOD CLASS 3 CA-<n> (for identity certificates)

or

cn=DOD CLASS 3 EMAIL CA-<n> (for identity certificates)

Here, **<n>** is a number. Numbers will be assigned sequentially to signing CAs as they are created. The complete DN for the root is:

cn=DOD CLASS 3 CA-<n>, ou=PKI, ou=DoD, o=U.S. Government, c=US

or

cn=DOD CLASS 3 EMAIL CA-<n>, ou=PKI, ou=DoD, o=U.S. Government, c=US

6.2.3 End-Entities

Except for CAs, all end-entities will be at level 6 of the DIT. These end-entities will have a common suffix that prefixes the organization to the base suffix. This common suffix is:

ou=<C/S/A>, ou=PKI, ou=DoD, o=U.S. Government, c=US

For example, the suffix for Army end-entities shall be:

ou=USA, ou=PKI, ou=DoD, o=U.S. Government, c=US

6.2.4 Registration Authorities

RAs shall be at level 6 of the DIT. The relative DN for the RA consists of adding a prefix to the RA's individual cn (See Section 6.2.6 below for a description of individual CNs). The format of the RA cn is:

cn=RA.<individual cn>

The complete DN for an RA is:

cn=RA.<individual cn>, ou=<C/S/A>, **ou=PKI, ou=DoD, o=U.S. Government, c=US**

An example DN for an RA is:

cn=RA.Smith.John.D.1234567890, ou=USA, **ou=PKI, ou=DoD, o=U.S. Government, c=US**

6.2.5 Local Registration Authorities

RAs shall be at level 6 of the DIT. The relative DN for the LRA consists of adding a prefix to the LRA's individual cn. The relative DN for the LRA is:

cn=LRA.<individual cn>

The complete DN for an LRA is:

cn=LRA.<individual cn>, ou=<C/S/A>, ou=PKI, ou=DoD, o=U.S. Government, c=US

An example DN for an LRA is:

cn=LRA.Jones.Alice.K.6789012345, ou=USA, ou=PKI, ou=DoD, o=U.S. Government, c=US

6.2.6 Individuals

A DN shall be created by the PKI for each user.

cn=<common name>, ou=<C/S/A>, ou=PKI, ou=DoD, o=U.S. Government, c=US

In user certificates issued by the DOD, the entire common name will not exceed 64 characters and will be unique. Applications should not assume a particular format for the common name. In current certificates, the common name consists of last name, generational qualifier, first name or initial, middle name or initial, and a ten-digit number, separated by periods; e.g., Smith.Jr.John.A.1234567890. Future releases may move the unique number to a separate attribute and make other changes to the format.

The name will be based on the name appearing on the individual's military or civilian ID card for military and DoD civilian personnel respectively and Social Security card or driver's license for non-DoD personnel.

6.2.7 Servers and Other Devices

Servers and other devices may require certificates to communicate with other entities. Servers and devices may operate autonomously without any direct human control. Devices include routers and switches. Servers and other devices shall be at level 6 of the DIT. The relative DN for a server or device is:

cn=<host name>

The host name is the server's domain name service (DNS) host name. The complete DN for a host is:

cn=<host name>, ou=<C/S/A>, ou=PKI, ou=DoD, o=U.S. Government, c=US

An example host name for a server sponsored by the Army is:

cn=www.mdw.army.mil, ou=USA, ou=PKI, ou=DoD, o=U.S. Government, c=US

Devices shall occur at level 6 of the DIT[80]. The format for device certificates may change as the requirements for IPSEC evolve.

[80] Devices are not currently being placed in the directory,

6.3 Object Classes

The previous section described the DN format for the various types of certificates. This section will describe the objects that the directory shall maintain. The objects described in this section are the objects that are visible to users of the PKI directory. The directory may contain other objects. These other objects may include objects predefined in the standard "default" schema of the products selected to implement the directory and objects used to provide other capabilities required in this specification. Examples of the latter class of objects are those implemented to manage consistency of directory information across a set of multiple, redundant directory servers.

Objects are hierarchically arranged. Subordinate objects inherit the attributes of their parent objects and may have additional attributes. Entries may belong to more than one object class. For each certificate, the directory contains an entry for the subject of the certificate. The DN of the directory entry will be identical to the subject name appearing in the certificate. Figure 6-2 illustrates the hierarchy.

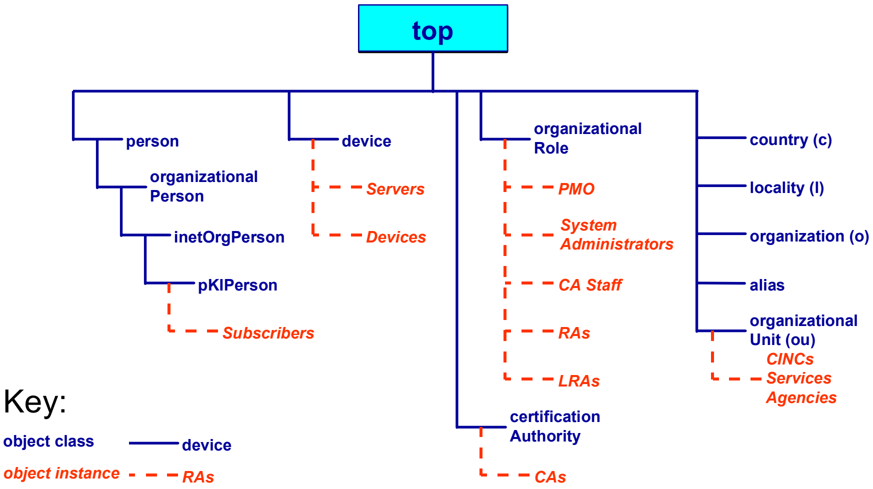

Figure 6-2. Directory Object Class Hierarchy

6.3.1 Certification Authority (CA)

CA directory objects for both the Root CA and signing CAs will contain attributes for the CA's certificate (issued by the Root CA) and the CA's most recently issued CRL. In the future the CA entry may include a cross certificate pair.

6.3.2 Individual Subscribers

Individual subscribers will belong to the pkiPerson class, which inherits from other classes: person, organizationalPerson, and inetOrgPerson. The inherited classes are standard object classes that provide the attributes for the "white page" information. The pkiPerson class provides attributes to uniquely identify users for purpose of preventing and resolving conflicts with associated UINs. Table 6-1 lists the attributes for the pkiPerson class. The responsibleLRA attribute contains the name of the subscriber's LRA when the subscriber has an active privacy key subject to key escrow.

Table 6-1. pkiPerson Attributes

pkiPerson Attributes
UIN
dateOfBirth
placeOfBirth
mothersMaidenName
effectiveServiceDate
responsibleLRA

6.3.3 PKI Roles

Personnel performing PKI functions must have directory entries that belong to the organizationalRole class. The directory must contain entries for individuals performing the functions listed in Table 6-2. The CN must include an indication of the role. The attributes of this class must specify the specific role and identify the individual occupying the role (roleOccupant). The description attribute will describe the individual's scope of responsibility (particularly for RAs and LRAs). An LRA might be responsible for a geographic region or a particular organization or group of organizations (within the DIT level 5 organization). The ou attribute will contain the same value as used in the entry's Level 5 component of the common name. Other OUs for appropriate subordinate organizations may also be present.

Table 6-2. Roles

Roles
PMO
System Administrator
CA Staff
Agency Focal Point
RA
LRA

6.3.4 Country

Since the DN structure associates only the value **US** with the country (**c**) element, this object class will only have one entry in the directory.

6.3.5 Organization

Since the DN structure associates the value **U.S. Government** with the organization (**o**) element at level 2 of the DIT, this objectclass will only have one entry in the directory.

6.3.6 Organizational Unit

The directory will include an **ou** object with the values **DOD** and **PKI** for Levels 3 and 4 respectively. The directory will have an **ou** entry for each of the C/S/A entries at level 5 of the directory. The required attributes for these Level 5 entries are:

Table 6-3. Level 5 Organizational Unit Required Attributes

Organizational Unit Required Attributes
description
seeAlso
st
l
telephoneNumber

The description attribute will contain the complete name of the organizational unit as listed in Appendix C. The seeAlso attribute will contain the common name of the organization's Agency FP.

6.3.7 Servers and Devices

Directory entries for servers and devices will belong to the device object class. The owner attribute will be a DN for the individual responsible for the device. The ou component will be the same as the level 5 DIT component of the object's DN.

6.4 Attributes

Appendix B contains a list of the attributes and their data type.

Appendix A

Object Identifiers

--id-rsa arc

```
pkcs-1::= { iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 }
rsaEncryption ::=  { pkcs-1 1}
sha1withRSAEncryption ::= {pkcs-1 5}
```

-- id-infosec arc

```
id-infosec ::= {joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) 1}
id-certificate-policy ::= {id-infosec 11}
id-US-dod-class3 ::= {id-certificate-policy 5}
id-US-dod-class4 ::= {id-certificate-policy 4}
id-US-dod-class5 ::= {id-certificate-policy 6}
id-US-medium-pilot ::= {id-certificate-policy 3}
id-US-dod-class3hardware ::= {id-certificate-policy 9}
reserved for future use ::= {id-certificate-policy 10}
```

-- PKIX Object Identifier Registry

```
id-pkix ::= { iso(1) identified-organization(3) dod(6) internet(1) security(5)
          mechanisms(5) pkix(7) }
```

-- PKIX Arcs

```
id-mod   ::= { id-pkix 0 }    -- modules
id-pe ::= { id-pkix 1 }    -- private certificate extensions
id-qt ::= { id-pkix 2 }    -- policy qualifier types
id-kp ::= { id-pkix 3 }    -- extended key purpose identifiers
id-it ::= { id-pkix 4 }    -- CMP information types
id-ct ::= { id-pkix 5 }    -- content types
id-alg ::= { id-pkix 6 }    -- algorithms
id-cmc ::= { id-pkix 7 }    -- CMC controls
id-on ::= { id-pkix 8 }    -- other name forms
id-pda ::= { id-pkix 9 }    -- personal data attribute
id-aca ::= { id-pkix 10 }   -- attribute certificate attributes
id-qcs ::= { id-pkix 11 }   -- qualified certificate statements
id-ad ::= { id-pkix 48 }   -- access descriptors
```

-- PKIX modules

```
id-pkix1-explicit-88 ::= { id-mod 1 }
id-pkix1-implicit-88 ::= { id-mod 2 }
id-pkix1-explicit-93 ::= { id-mod 3 }
id-pkix1-implicit-93 ::= { id-mod 4 }
```

```
    id-mod-crmf ::= { id-mod 5 }
    id-mod-cmc ::= { id-mod 6 }
    id-mod-kea-profile-88 ::= { id-mod 7 }
    id-mod-kea-profile-93 ::= { id-mod 8 }
    id-mod-cmp ::= { id-mod 9 }
    id-mod-qualified-cert-88 ::= { id-mod 10 }
    id-mod-qualified-cert-93 ::= { id-mod 11 }
    id-mod-attribute-cert ::= { id-mod 12 }
    id-mod-ocsp ::= { id-mod 14 }

-- PKIX private extensions

    id-pe-authorityInfoAccess ::= { id-pe 1 }
    id-pe-biometricInfo ::= { id-pe 2 }
    id-pe-qcStatements ::= { id-pe 3 }
    id-pe-ac-auditIdentity ::= { id-pe 4 }
    id-pe-ac-targeting ::= { id-pe 5 }
    id-pe-aaControls ::= { id-pe 6 }

-- policyQualifierIds for Internet policy qualifiers

    id-qt-cps ::= { id-qt 1 }
    id-qt-unotice ::= { id-qt 2 }
    id-qt-textNotice ::= { id-qt 3 }

-- content types

    id-ct-crs ::= { id-ct 1 }
    id-ct-PKIData ::= { id-ct 2 }
    id-ct-PKIResponse ::= { id-ct 3 }

-- algorithms

    id-alg-des40 ::= { id-alg 1 }
    id-alg-noSignature ::= { id-alg 2 }
    id-alg-dh-sig-hmac-sha1 ::= { id-alg 3 }
    id-alg-dh-pop ::= { id-alg 4 }

-- CMC controls

    id-cmc-statusInfo ::= { id-cmc 1 }
    id-cmc-identification ::= { id-cmc 2 }
    id-cmc-identityProof ::= { id-cmc 3 }
    id-cmc-dataReturn ::= { id-cmc 4 }
    id-cmc-transactionId ::= { id-cmc 5 }
    id-cmc-senderNonce ::= { id-cmc 6 }
    id-cmc-recipientNonce ::= { id-cmc 7 }
    id-cmc-addExtensions ::= { id-cmc 8 }
    id-cmc-encryptedPOP ::= { id-cmc 9 }
    id-cmc-decryptedPOP ::= { id-cmc 10 }
    id-cmc-lraPOPWitness ::= { id-cmc 11 }
    id-cmc-getCert ::= { id-cmc 15 }
    id-cmc-getCRL ::= { id-cmc 16 }
    id-cmc-revokeRequest ::= { id-cmc 17 }
    id-cmc-regInfo ::= { id-cmc 18 }
    id-cmc-responseInfo ::= { id-cmc 19 }
    id-cmc-queryPending ::= { id-cmc 21 }
    id-cmc-popLinkRandom ::= { id-cmc 22 }
    id-cmc-popLinkWitness ::= { id-cmc 23 }
    id-cmc-confirmCertAcceptance ::= { id-cmc 24 }

-- access descriptors for authority info access extension

    id-ad-ocsp ::= { id-ad 1 }
    id-ad-caIssuers ::= { id-ad 2 }

-- ocsp OIDs

    id-kp-OCSPSigning ::= { id-kp 9 }
    id-pkix-ocsp ::= { id-ad-ocsp }
    id-pkix-ocsp-basic ::= { id-pkix-ocsp 1 }
    id-pkix-ocsp-nonce ::= { id-pkix-ocsp 2 }
    id-pkix-ocsp-crl  ::= { id-pkix-ocsp 3 }
    id-pkix-ocsp-response ::= { id-pkix-ocsp 4 }
    id-pkix-ocsp-nocheck ::= { id-pkix-ocsp 5 }
    id-pkix-ocsp-archive-cutoff ::= { id-pkix-ocsp 6 }
    id-pkix-ocsp-service-locator ::= { id-pkix-ocsp 7 }
```

Appendix B

Directory Objects and Attributes

```
# The format of this file is:
#
#  objectclass ObjectClassName
#       [ oid ObjectIdentifier ]
#       [ superior ParentObjectClass ]
#       [ requires <comma separated list of required attributes> ]
#       [ allows   <comma separated list of allowed attributes>  ]
#
```

B.1 Object Classes

```
objectclass top
        oid 2.5.6.0
        requires
                objectClass
        allows
                aci

objectclass alias
        oid 2.5.6.1
        superior top
        requires
                aliasedObjectName

objectclass country
        oid 2.5.6.2
        superior top
        requires
                c
        allows
                searchGuide,
                description

objectclass locality
```

```
    oid 2.5.6.3
    superior top
    allows
        description,
        l,
        searchGuide,
        seeAlso,
        st,
        street

objectclass organization
    oid 2.5.6.4
    superior top
    requires
        o
    allows
        businessCategory,
        description,
        destinationIndicator,
        facsimileTelephoneNumber,
        internationaliSDNNumber,
        l,
        physicalDeliveryOfficeName,
        postOfficeBox,
        postalAddress,
        postalCode,
        preferredDeliveryMethod,
        registeredAddress,
        searchGuide,
        seeAlso,
        st,
        street,
        telephoneNumber,
        teletexTerminalIdentifier,
        telexNumber,
        userPassword,
        x121Address

objectclass organizationalUnit
    oid 2.5.6.5
    superior top
```

```
        requires
                ou
        allows
                businessCategory,
                description,
                destinationIndicator,
                facsimileTelephoneNumber,
                internationaliSDNNumber,
                l,
                physicalDeliveryOfficeName,
                postOfficeBox,
                postalAddress,
                postalCode,
                preferredDeliveryMethod,
                registeredAddress,
                searchGuide,
                seeAlso,
                st,
                street,
                telephoneNumber,
                teletexTerminalIdentifier,
                telexNumber,
                userPassword,
                x121Address

objectclass person
        oid 2.5.6.6
        superior top
        requires
                sn,
                cn
        allows
                description,
                seeAlso,
                telephoneNumber,
                userPassword

objectclass organizationalPerson
        oid 2.5.6.7
        superior person
        allows
```

```
                destinationIndicator,
                facsimileTelephoneNumber,
                internationaliSDNNumber,
                l,
                ou,
                physicalDeliveryOfficeName,
                postOfficeBox,
                postalAddress,
                postalCode,
                preferredDeliveryMethod,
                registeredAddress,
                st,
                street,
                teletexTerminalIdentifier,
                telexNumber,
                title,
                x121Address

objectclass inetOrgPerson
   oid 2.16.840.1.113730.3.2.2
   superior organizationalPerson
         allows
                audio,
                businessCategory,
                carLicense,
                departmentNumber,
                employeeType,
                employeeNumber,
                givenName,
                homePhone,
                homePostalAddress,
                initials,
                jpegPhoto,
                labeledURI,
                manager,
                mobile,
                pager,
                photo,
                preferredLanguage,
                mail,
                roomNumber,
                        secretary,
                        uid,
                        x500uniqueIdentifier,
                        userCertificate,
                        userCertificate;binary,
                        userSMimeCertificate;binary

objectclass pkiPerson
    oid TBD
    superior organizationalPerson
            requires
                        UIN
                        dateOfBirth,
                        placeOfBirth,
                        mothersMaidenName,
                        effectiveServiceDate,
allows
                        responsibleLRA

objectclass organizationalRole
   oid 2.5.6.8
   superior top
            requires
                        cn
            allows
                        description,
                        destinationIndicator,
                        facsimileTelephoneNumber,
                        internationaliSDNNumber,
                        l,
                        ou,
                        physicalDeliveryOfficeName,
                        postOfficeBox,
                        postalAddress,
                        postalCode,
                        preferredDeliveryMethod,
                        registeredAddress,
                        roleOccupant,
                        seeAlso,
                        st,
                        street,
                        telephoneNumber,
                        teletexTerminalIdentifier,
                        telexNumber,
                        x121Address

objectclass groupOfCertificates
    oid 2.16.840.1.113730.3.2.31
    superior top
            requires
                        cn
            allows
                        memberCertificateDescription,
                        businessCategory,
                        description,
                        o,
                        ou,
                        owner,
                        seeAlso

objectclass device
    oid 2.5.6.14
    superior top
            requires
                        cn
            allows
                        description,
                        l,
                        o,
                        ou,
                        owner,
                        seeAlso,
                        serialNumber

objectclass certificationAuthority
    oid 2.5.6.16
    superior top
            requires
                        cACertificate;binary
            allows
                        authorityRevocationList;binary,
                        certificateRevocationList;binary,
                        crossCertificatePair;binary

objectclass domain
    oid 0.9.2342.19200300.100.4.13
    superior top
            requires
                        dc
            allows
                        associatedName,
                        businessCategory,
                        description,
                        destinationIndicator,
                        facsimileTelephoneNumber,
                        internationaliSDNNumber,
                        l,
                        manager,
                        o,
                        physicalDeliveryOfficeName,
                        postOfficeBox,
                        postalAddress,
                        postalCode,
                        preferredDeliveryMethod,
                        registeredAddress,
                        searchGuide,
                        seeAlso,
                        st,
                        street,
                        telephoneNumber,
                        teletexTerminalIdentifier,
                        telexNumber,
                        userPassword,
                        x121Address

objectclass RFC822localPart
    oid 0.9.2342.19200300.100.4.14
    superior domain
            allows
                        cn,
                        sn

objectclass DNSDomain
```

```
  oid 0.9.2342.19200300.100.4.15
  superior domain
       allows
              dNSRecord

objectclass labeledURIObject
       oid 1.3.6.1.4.1.250.3.15
       superior top
       allows
              labeledURI
```

B.2 Attributes

Table B-1 Directory Attributes

Attribute Name	Alternate Name	Object Identifier	Type
abstract		abstract-oid	cis
aci		2.16.840.1.113730.3.1.55	bin
administratorContactInfo		2.16.840.1.113730.3.1.74	cis
adminUrl		2.16.840.1.113730.3.1.75	ces
aliasedObjectName		2.5.4.1	dn
altServer		1.3.6.1.4.1.1466.101.120.6	ces
associatedDomain		0.9.2342.19200300.100.1.37	cis
associatedName		0.9.2342.19200300.100.1.38	dn
attributeTypes		2.5.21.5	cis
audio		0.9.2342.19200300.100.1.55	bin
authorCn	documentauthorcommonname	authorcn-oid	cis
authorityRevocationList;binary	authorityRevocationList	2.5.4.38	bin
authorSn	documentauthorsurname	authorsn-oid	cis
buildingName		0.9.2342.19200300.100.1.48	cis
businessCategory		2.5.4.15	cis
c	countryName	2.5.4.6	cis
cACertificate;binary	cACertificate	2.5.4.37	bin
carLicense		2.16.840.1.113730.3.1.1	cis
certificateRevocationList;binary	certificateRevocationList	2.5.4.39	bin
changeLog		2.16.840.1.113730.3.1.35	dn
changeLogMaximumAge		2.16.840.1.113730.3.1.200	cis
changeLogMaximumSize		2.16.840.1.113730.3.1.201	cis
changeNumber		2.16.840.1.113730.3.1.5	int
changes		2.16.840.1.113730.3.1.8	bin
changeTime		2.16.840.1.113730.3.1.77	cis

Attribute Name	Alternate Name	Object Identifier	Type
changeType		2.16.840.1.113730.3.1.7	cis
cirBeginORC		2.16.840.1.113730.3.1.90	cis
cirBindCredentials		2.16.840.1.113730.3.1.85	ces
cirBindDn		2.16.840.1.113730.3.1.82	dn
cirHost		2.16.840.1.113730.3.1.80	cis
cirLastUpdateApplied		2.16.840.1.113730.3.1.86	cis
cirPort		2.16.840.1.113730.3.1.81	cis
cirReplicaRoot		2.16.840.1.113730.3.1.79	dn
cirSyncInterval		2.16.840.1.113730.3.1.89	cis
cirUpdateFailedat		2.16.840.1.113730.3.1.88	cis
cirUpdateSchedule		2.16.840.1.113730.3.1.87	cis
cirUsePersistentSearch		2.16.840.1.113730.3.1.83	cis
cirUseSsl		2.16.840.1.113730.3.1.84	cis
cn	commonName	2.5.4.3	cis
co	friendlycountryname	0.9.2342.19200300.100.1.43	cis
createTimestamp		2.5.18.1	cis
creatorsName		2.5.18.3	dn
crossCertificatePair;binary	crossCertificatePair	2.5.4.40	bin
dc	domaincomponent	0.9.2342.19200300.100.1.25	cis
deleteOldRdn		2.16.840.1.113730.3.1.10	cis
deltaRevocationList;binary		2.5.4.53	bin
departmentNumber		2.16.840.1.113730.3.1.2	cis
description		2.5.4.13	cis
destinationIndicator		2.5.4.27	cis
dITContentRules		2.5.21.2	cis
ditRedirect		0.9.2342.19200300.100.1.54	dn
dITStructureRules		2.5.21.1	cis
dn	distinguishedName	2.5.4.49	dn
dnQualifier		2.5.4.46	cis
dNSRecord		0.9.2342.19200300.100.1.26	cis
documentAuthor		0.9.2342.19200300.100.1.14	dn
documentIdentifier		0.9.2342.19200300.100.1.11	cis
documentLocation		0.9.2342.19200300.100.1.15	cis
documentPublisher		0.9.2342.19200300.100.1.56	cis
documentPublisher		0.9.2342.19200300.100.1.56	cis
documentStore		documentStore-oid	cis
documentTitle		0.9.2342.19200300.100.1.12	cis
documentVersion		0.9.2342.19200300.100.1.13	cis
drink		0.9.2342.19200300.100.1.5	cis
dSAQuality		0.9.2342.19200300.100.1.49	cis

Attribute Name	Alternate Name	Object Identifier	Type
employeeNumber		2.16.840.1.113730.3.1.3	cis
employeeType		2.16.840.1.113730.3.1.4	cis
enhancedSearchGuide		2.5.4.47	cis
facsimileTelephoneNumber	fax	2.5.4.23	tel
filterInfo		2.16.840.1.113730.3.1.206	cis
generation		generation-oid	ces
generationQualifier		2.5.4.44	cis
givenName		2.5.4.42	cis
homePhone		0.9.2342.19200300.100.1.20	tel
homePostalAddress		0.9.2342.19200300.100.1.39	cis
host		0.9.2342.19200300.100.1.9	cis
houseIdentifier		2.5.4.51	cis
info		0.9.2342.19200300.100.1.4	cis
initials		2.5.4.43	cis
installationTimeStamp		2.16.840.1.113730.3.1.73	cis
internationalIsdnNumber		2.5.4.25	ces
janetMailbox		0.9.2342.19200300.100.1.46	cis
jpegPhoto		0.9.2342.19200300.100.1.60	bin
keyWords		keyWords-oid	cis
knowledgeInformation		2.5.4.2	cis
l	locality localityname,	2.5.4.7	cis
lastModifiedBy		0.9.2342.19200300.100.1.24	dn
lastModifiedTime		0.9.2342.19200300.100.1.23	cis
ldapSyntaxes		1.3.6.1.4.1.1466.101.120.16	cis
mail	rfc822mailbox	0.9.2342.19200300.100.1.3	cis
mailPreferenceOption		0.9.2342.19200300.100.1.47	int
manager		0.9.2342.19200300.100.1.10	dn
matchingRules		2.5.21.4	cis
matchingRuleUse		2.5.21.8	cis
member		2.5.4.31	dn
memberCertificateDescription		2.16.840.1.113730.3.1.199	ces
memberURL		2.16.840.1.113730.3.1.198	ces
mobile	mobileTelephoneNumber	0.9.2342.19200300.100.1.41	tel
modifiersName		2.5.18.4	dn
modifyTimestamp		2.5.18.2	cis
multiLineDescription		multiLineDescription-oid	cis
nameForms		2.5.21.7	cis
namingContexts		1.3.6.1.4.1.1466.101.120.5	dn
newRdn		2.16.840.1.113730.3.1.9	dn
newSuperior		2.16.840.1.113730.3.1.11	dn

Attribute Name	Alternate Name	Object Identifier	Type
nsLicensedFor		2.16.840.1.113730.3.1.36	cis
nsLicenseEndTime		2.16.840.1.113730.3.1.38	cis
nsLicenseStartTime		2.16.840.1.113730.3.1.37	cis
o	organizationname	2.5.4.10	cis
objectClass		2.5.4.0	cis
objectClasses		2.5.21.6	cis
obsoletedByDocument		obsoletedByDocument-oid	dn
obsoletesDocument		obsoletesDocument-oid	dn
organizationalStatus		0.9.2342.19200300.100.1.45	cis
otherMailbox		0.9.2342.19200300.100.1.22	cis
ou	organizationalUnitName	2.5.4.11	cis
owner		2.5.4.32	dn
pager	pagerTelephoneNumber	0.9.2342.19200300.100.1.42	tel
personalSignature		0.9.2342.19200300.100.1.53	bin
personalTitle		0.9.2342.19200300.100.1.40	cis
photo		0.9.2342.19200300.100.1.7	bin
physicalDeliveryOfficeName		2.5.4.19	cis
postalAddress		2.5.4.16	cis
postalCode		2.5.4.17	cis
postOfficeBox		2.5.4.18	cis
preferredDeliveryMethod		2.5.4.28	cis
preferredLanguage		2.16.840.1.113730.3.1.39	cis
presentationAddress		2.5.4.29	ces
protocolInformation		2.5.4.48	cis
reciprocalNamingLink		reciprocalNaminglink-oid	dn
ref		2.16.840.1.113730.3.1.34	ces
registeredAddress		2.5.4.26	cis
replicaBeginOrc		2.16.840.1.113730.3.1.50	cis
replicaBindDn		2.16.840.1.113730.3.1.58	dn
replicaBindMethod		2.16.840.1.113730.3.1.53	cis
replicaCredentials		2.16.840.1.113730.3.1.202	bin
replicaEntryFilter		2.16.840.1.113730.3.1.203	ces
replicaHost		2.16.840.1.113730.3.1.197	cis
replicaNickName		2.16.840.1.113730.3.1.204	cis
replicaPort		2.16.840.1.113730.3.1.48	cis
replicaRoot		2.16.840.1.113730.3.1.57	dn
replicaUpdateFailedAt		2.16.840.1.113730.3.1.49	cis
replicaUpdateReplayed		2.16.840.1.113730.3.1.51	cis
replicaUpdateSchedule		2.16.840.1.113730.3.1.52	cis
replicaUseSSL		2.16.840.1.113730.3.1.54	cis

Attribute Name	Alternate Name	Object Identifier	Type
roleOccupant		2.5.4.33	dn
roomNumber		0.9.2342.19200300.100.1.6	cis
searchGuide		2.5.4.14	ces
secretary		0.9.2342.19200300.100.1.21	dn
seeAlso		2.5.4.34	dn
serialNumber		2.5.4.5	cis
serverHostName		2.16.840.1.113730.3.1.76	cis
serverProductName		2.16.840.1.113730.3.1.71	cis
serverRoot		2.16.840.1.113730.3.1.70	cis
serverVersionNumber		2.16.840.1.113730.3.1.72	cis
singleLevelQuality		0.9.2342.19200300.100.1.50	cis
sn	surName	2.5.4.4	cis
st	stateOrProvinceName	2.5.4.8	
street	streetaddress	2.5.4.9	cis
subject		subject-oid	cis
subschemaSubentry		2.5.18.10	dn
subtreeACI		2.16.840.1.113730.3.1.69	ces
subtreeMaximumQuality		0.9.2342.19200300.100.1.52	cis
subtreeMinimumQuality		0.9.2342.19200300.100.1.51	cis
supportedAlgorithms;binary		2.5.4.52	bin
supportedApplicationContext		2.5.4.30	cis
supportedControl		1.3.6.1.4.1.1466.101.120.13	cis
supportedExtension		1.3.6.1.4.1.1466.101.120.7	cis
supportedLDAPVersion		1.3.6.1.4.1.1466.101.120.15	int
supportedSASLMechanisms		1.3.6.1.4.1.1466.101.120.14	cis
targetDn		2.16.840.1.113730.3.1.6	dn
telephoneNumber		2.5.4.20	tel
teletexTerminalIdentifier		2.5.4.22	cis
telexNumber		2.5.4.21	cis
textEncodedORAddress		0.9.2342.19200300.100.1.2	cis
title		2.5.4.12	cis
ttl	timeToLive	1.3.6.1.4.1.250.1.60	cis
uid		0.9.2342.19200300.100.1.1	cis
uniqueIdentifier		0.9.2342.19200300.100.1.44	cis
uniqueMember		2.5.4.50	dn
updatedByDocument		updatedByDocument-oid	dn
updatesDocument		updatesDocument-oid	dn
userCertificate;binary	userCertificate	2.5.4.36	bin
userClass		0.9.2342.19200300.100.1.8	cis
userPassword		2.5.4.35	bin

Attribute Name	Alternate Name	Object Identifier	Type
userSMIMECertificate;binary		2.16.840.1.113730.3.1.40	bin
x121Address		2.5.4.24	ces
x500UniqueIdentifier		2.5.4.45	bin

Appendix C

DOD PKI URIs

C.1 HTTP URIs

User Registration Page

http://reg.c3pki.chamb.disa.mil

http://reg.c3pki.den.disa.mil

RA/LRA Pages

http://admin.c3pki.chamb.disa.mil

http://admin.c3pki.den.disa.mil

PKI Home Page

http://dodpki.c3pki.chamb.disa.mil

http://dodpki.c3pki.den.disa.mil

HTTP access to Directories

http://ds-web.c3pki.chamb.disa.mil/id

http://ds-web.c3pki.chamb.disa.mil/mail

http://ds-web.c3pki.den.disa.mil/id

http://ds-web.c3pki.den.disa.mil/mail

HTTP Access to CRLs

http://ca-3.c3pki.chamb.disa.mil (CRL list for Identity and Server Certificates issued by Chambersburg)

http://ca-4.c3pki.den.disa.mil (CRL list for Identity and Server Certificates issued by Denver)

http://email-ca-3.c3pki.chamb.disa.mil (CRL list for Email Certificates issued by Chambersburg)

http://email-ca-4.c3pki.den.disa.mil (CRL list for Email Certificates issued by Denver)

After getting to the appropriate CA, perform the following steps to retrieve a CRL for Netscape browsers:

- click Retrieval tab
- select Import Certificate Revocation List
- select Import the latest CRL to your browser (radio button)
  click Submit

OCSP Validation (planned for PKI version 3.0)

http://ocsp.c3pki.chamb.disa.mil

http://ocsp.c3pki.den.disa.mil

C.2 LDAP Access

This section describes how one can gain access to certificates in DOD PKI directories. There are a number of LDAP clients available, each with a unique user interface. In general, there needs to be:

- Action (search, modify, delete)
- URL – host where the directory server resides
- Base DN – point in directory hierarchy to begin search
- Filter – criteria for matching (e.g., user ID or Common Name)
- Attributes – those attributes of interest

In the DOD PKI release 2.0, there will be two primary directories (one for identity certificates and one for email certificates). There will also be replicated directories for each. Also, for a transition period, the DOD PKI version 1.0 directories will remain operational. The following URLs will be available:

Table C-1. DOD Directory URLs

Purpose	URL[81]
Primary Identity	**ldap://ds-3.c3pki.chamb.disa.mil**
Primary Identity (LDAP over SSL)	**ldaps:// ds-3.c3pki.chamb.disa.mil[82]**
Replica Identity	**ldap://ds-4.c3pki.den.disa.mil**
Primary Email	**ldap://email-ds-3.c3pki.chamb.disa.mil**
Primary Email (LDAP over SSL)	**ldaps://email-ds-3.c3pki.chamb.disa.mil:687[83]**
Replica Email	**ldap://email-ds-4.c3pki.den.disa.mil**

One of the above URLs, as appropriate, will be used with the following Base DN, Filter, and Attributes sought combinations.

Table C-2. LDAP Paramaters for Obtaining PKI Objects

Purpose	Base DN	Filter	Attributes Sought
Root Certificate	ou=PKI, ou=DOD, o=U.S. Government, c=US	cn=DoD CLASS 3 Root CA	caCertificate;binary
Identity CA Certificate	ou=PKI, ou=DOD, o=U.S. Government, c=US	cn=DOD CLASS 3 CA-<3|4>[84]	caCertificate;binary
Email CA Certificate	ou=PKI, ou=DOD,	cn=DOD CLASS 3	caCertificate;binary

[81] Standard ports (389 for LDAP, 686 for LDAP over SSL) are used unless otherwise noted

[82] Both LDAP over SSL and LDAP are offered at Chambersburg. SSL is primarily needed for updates.

[83] In the current architecture, the email LDAP over SSL needs to operate over a non-standard port. This is expected to be fixed when PKI Release 3.0 is deployed at which time the standard port (686) will be used.

[84] CA-3 is in Chambersburg; CA-4 is in Denver; Additional CAs may be added in the future as performance necessitates

	o=U.S. Government, c=US	EMAIL CA-<3|4>	
Identity Certificate	ou=<C/S/A/C>,[85] ou=PKI, ou=DOD, o=U.S. Government, c=US	cn=<user common name>	userCertificate;binary
Email Certificate	ou=<C/S/A/C>, ou=PKI, ou=DOD, o=U.S. Government, c=US	cn=<user common name>	userCertificate;binary
CRL for Root and CAs	ou=<C/S/A/C>, ou=PKI, ou=DOD, o=U.S. Government, c=US	cn=DoD CLASS 3 Root CA	CertificateRevocation List;binary
CRL for User Identity Certificates	o=PKI, ou=DOD, o=U.S. Government, c=US	cn=DOD CLASS 3 EMAIL CA-<3|4>	CertificateRevocation List;binary
CRL for User Email Certificates	o=PKI, ou=DOD, o=U.S. Government, c=US	cn=DOD CLASS 3 EMAIL CA-<3|4>	CertificateRevocation List;binary

[85] "C/S/A/C" stands for CINC, Service, Agency, or Contractor

Appendix D

DOD Organizations

The following table lists the organizations comprising the level immediately below the directory suffix. The categories (CINCS, Services, Agencies, and Field Activities) are for presentation only and would not appear as entries. The values shown in the Directory Entry column would appear as the organization unit (ou) component in the directory.

Directory suffix:

ou=PKI, ou=DoD, o=U.S. Government, c=US

Example:

All Army entries would share the common suffix:
ou=USA, ou=PKI, ou=DoD, o=U.S. Government, c=US

Table 1 PKI Organizational Units

Organization	Directory Entry
Unified Combatant Commands	
Atlantic Command[86]	ACOM
Central Command	CENTCOM
European Command	EUCOM
Joint Forces Command	JFCOM
Pacific Command	PACOM
Southern Command	SOUTHCOM
Space Command	SPACECOM
Special Operations Command	SOCOM
Strategic Command	STRATCOM

[86] Has been replaced by JFCOM. Should not appear on new certificates

Organization	Directory Entry
Transportation Command	TRANSCOM
Services	
US Army	USA
US Navy	USN
US Air Force	USAF
US Marines	USMC
US Coast Guard (non-DOD)	USCG
Defense Agencies	
Ballistic Missile Defense Office	BMDO
Defense Advanced Research Projects Agency	DARPA
Defense Commissary Agency	DeCA
Defense Contract Audit Agency	DCAA
Defense Contract Management Agency	DCMA
Defense Finance and Accounting Agency	DFAS
Defense Information Systems Agency	DISA
Defense Intelligence Agency	DIA
Defense Legal Services Agency	DLSA
Defense Logistics Agency	DLA
Defense Security Assistance Agency[87]	DSAA
Defense Security Cooperation Agency	DSCA
Defense Security Service	DSS
Defense Special Weapons Agency[88]	DSWA

[87] Has been replaced by Defense Security Cooperation Agency. Should not appear on new certificates

Organization	Directory Entry
Defense Threat Reduction Agency	DTRA
On-Site Inspection Agency[89]	OSIA
National Imagery and Mapping Agency	NIMA
National Security Agency/Central Security Service	NSA/CSS
DoD Field Activities	
American Forces Information Services	AFIS
Defense Medical Programs Activity[90]	DMPA
Defense POW/MP Office	POW/MP
Defense Technology Security Administration[91]	DTSA
DoD Education Activity	DoDEA[92]
DoD Human Resources Activity	HRA
Office of Civilian Health & Medical Program of the Uniformed Services[93]	OCHAMPUS
Office of Economic Adjustment	OEA
Tricare Management Activity	TMA
Washington Headquarters Services	WHS

[88] Eliminated?

[89] Has been replaced by Defense Threat Reduction Agency. Should not appear on new certificates

[90] Has been absorbed into Tricare Management Activity. Should not appear on new certificates

[91] Eliminated? Should not appear

[92] Older certificates may have the acronym DEA

[93] Has been absorbed into Tricare Management Activity. Should not appear on new certificates

List of References

DISA, *Department of Defense (DOD) Medium Assurance Public Key Infrastructure (PKI) Functional Specification,* Draft, 20 October 1998.

DISA, *Department of Defense (DOD) Class 3 PKI Concept of Operations,* December 1999.

IETF, *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, January 1999, RFC 2459.

RSA, *PKCS #1: RSA Cryptography Standard*, Version 2.0, September1998.

RSA, *PKCS #7: Cryptographic Message Syntax Standard*, Version 1.5, November 1993.

RSA, *PKCS #10: Certification Request Syntax Standard,* Version 1.0, November 1993.

RSA, *PKCS #12: Personal Information Exchange Syntax Standard*, Version 1.0 June 1999.